Preventing Attacks by Improving Intelligence

Good intelligence used effectively is the key to preventing terrorist attacks. While the intelligence failures leading up to the September 11, 2001, attacks have been well documented, major shortcomings continue to frustrate intelligence efforts. New intelligence capabilities, such as a comprehensive and integrated terrorist watch list, are not yet in place, and old problems, such as insufficient sharing of terrorist threat intelligence, remain. To remedy these shortcomings, the Administration should clarify the mission of the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, complete a comprehensive strategic threat and vulnerability assessment to prioritize protective measures and guide homeland security strategic planning, and improve the sharing of information among federal agencies, with state and local governments and with the private sector.

The bipartisan Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (Congressional Joint Inquiry) stated that the U.S. government was unable to prevent the al Qaeda attacks due to failures in collecting intelligence, assembling and analyzing the information that was collected, placing suspected terrorists on watch lists, understanding the terrorist threat as it related to specific U.S. security vulnerabilities, and sharing information across government agencies and with state and local authorities.[1]

These failures suggest that defeating the threat of terrorism requires a new and different type of intelligence structure than was needed during the Cold War or for past military operations. The challenge now is to understand a terrorist threat that is decentralized, with small cells of operatives focused on attacking non-traditional targets such as airliners or other civilian infrastructure. Our government needs to be equally agile in "connecting the dots," and sharing information collected from disparate sources with those in place to prevent terrorist attacks.[2]

SECURITY GAP: The Directorate of Information Analysis and Infrastructure Protection Suffers From an Unclear Mission and Insufficient Resources.

Congress sought to address the intelligence failures of September 11, 2001 and provide an effective counterterrorism intelligence unit when it created the Department of Homeland Security

---

[1] House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, House Report 107-792 and Senate Report 107-351, December, 2002.

[2] See, for example, (a) Markle Foundation, *Protecting America's Freedom in the Information Age*, (New York: Markle Foundation, October, 2002); (b) James B. Steinberg, Mary Graham, and Andrew Eggers, "Building Intelligence to Fight Terrorism," *the Brookings Institution*, September 2003; (c) Kevin O'Connell and Robert R. Tomes, "Keeping the Information Edge," *Policy Review*, December 2003; and (d) Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Fifth Annual Report to the President and Congress.* (Arlington, VA: RAND, December 15, 2003).

(DHS) Directorate of Information Analysis and Infrastructure Protection (IAIP). Consistent with the 2002 Homeland Security Act, the IAIP Directorate is charged with analyzing intelligence related to the terrorist threat on the homeland; mapping the terrorist threat to specific vulnerabilities; conducting assessments of the terrorist threats and vulnerabilities in order to make appropriate recommendations for prioritizing security efforts according to threat; disseminating intelligence to federal, state, and local officials to improve prevention measures; and conducting threat alerts.[3]

Since the passage of the Homeland Security Act, however, the key task of assembling, analyzing, and assessing intelligence related to the terrorist threat on the homeland has been taken over by the Terrorist Threat Integration Center (TTIC). The President announced the creation of TTIC in January, 2003, during the State of the Union Address as the center for terrorist-related threat analysis and assessments.[4] The TTIC is currently a "joint venture" between the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and DHS, with a director that reports to the Director of Central Intelligence. Additionally, consistent with the mandate of the Homeland Security Act, responsibility for operating a comprehensive government terrorist watch list previously had been assigned to DHS. However, the task of compiling and administering such a watch list has now been assumed by the Terrorist Screening Center (TSC), which is part of the FBI.[5]

Moreover, the FBI's own Counter Terrorism Division has expanded dramatically since September 11, 2001, and it has assumed some of the responsibilities that Congress placed within DHS for intelligence analysis and information sharing.[6] The Department of Defense's newly created Northern Command also boasts an intelligence fusion center that analyzes and disseminates information on threats to the homeland.

The creation of TTIC and TSC and the expansion of intelligence functions within previously existing agencies has led to confusion about the central mission of the IAIP Directorate. While it still seeks to map terrorist threats against U.S. vulnerabilities and disseminate threat information to state and local officials, it is no longer in a position to act as the federal government's central fusion center to receive and analyze all terrorist threat-related information as envisioned by the Homeland Security Act. It cannot serve as the main entity to "connect the dots," as was called for in the aftermath of September 11, 2001, but must instead coexist with other intelligence agencies who have now assumed one of its key intended functions. According to the DHS Inspector General, the TTIC and TSC "either overlap with, duplicate, or even trump [the authorities] of IAIP. Ensuring that DHS has access to the intelligence that it needs to prevent and/or respond to

---

[3] "Homeland Security Act of 2002." (P.L. 107-296, §201).
[4] The White House, "Strengthening Intelligence to Better Protect America," February 14, 2003. http://www.whitehouse.gov/news/releases/2003/02/20030214-1.html.
[5] The White House, "New Terrorist Screening Center Established," September 16, 2003. http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html.
[6] According to House Report 108-401 accompanying the Omnibus Appropriations Act for fiscal year 2004, 523, "Since the terrorist attacks on September 11th, 2001, the FBI has shifted its main focus from investigating crimes to preventing acts of terrorism. Inherent in this transformation is a greater emphasis on collection, management, and analysis of data and intelligence, and greater collaboration across all levels of law enforcement. The urgency to prevent acts of terrorism has required the infusion of substantial resources, with the FBI growing by over 50 percent in just three years."

terrorist threats is, under such circumstances, an even harder challenge than it would otherwise be."[7]

Compounding the IAIP Directorate's inability to carry out one of its central missions is its current shortage of resources. Although Congress approved funds for 692 employees for the Directorate for fiscal year 2004, fewer than 300 people had been hired as of February 11, 2004.[8] This has translated into fewer personnel available to serve in liaison positions at other intelligence entities. For example, as of November 20, 2003, DHS had assigned only five full-time analysts to TTIC of the 30 to 45 projected to be necessary.[9] Also, in a broader budget context, the President's fiscal year 2005 budget proposes that DHS will no longer contribute any funding to TTIC and the TSC, as is currently being done.[10] Given that budget authority can equate to influence in ensuring that it receives the intelligence information required to prevent and respond to terrorists threat, DHS, under such circumstances, potentially faces additional barriers to fulfilling its mission.

SECURITY RECOMMENDATION

The Administration should take steps to reinvigorate the IAIP Directorate in recognition of its central role in fulfilling a core function of the Department of Homeland Security. Specifically, it should clarify the mission of the Directorate in light of the creation of the TTIC and the TSC and the expansion of terrorist threat analysis functions of other government agencies and ensure that the Directorate has the full range of staffing, technological, and physical resources necessary to carry out its legally mandated duties. The Administration should propose amendments, if needed, to the Homeland Security Act to clarify IAIP's missions and responsibilities The Administration should also ensure that the IAIP Directorate receives access to all intelligence information it may require in carrying out its responsibilities under the Homeland Security Act, despite any future funding arrangements for the TTIC and TSC.

---

[7] Department of Homeland Security, Office of Inspector General, "Major Management Challenges Facing the Department of Homeland Security," December 31, 2003, 6. http://www.dhs.gov/interweb/assetlibrary/FY04managementchallenges.pdf.

[8] Briefing by IAIP staff for staff of the House Select Committee on Homeland Security, February 13, 2004. An additional 100 personnel are in the process of being hired by the Directorate. The President's fiscal year 2005 request seeks no significant increase in personnel for the IAIP Directorate.

[9] John O. Brennan, Director, Terrorist Threat Integration Center. December 4, 2003. Response to Questions for the Record, Joint hearing of the House Select Committee on Homeland Security and House Judiciary Committee, "The Terrorist Threat Integration Center and its relationship with the Departments of Justice and Homeland Security." July 22, 2003.

[10] According to Administration fiscal year 2005 budget request documents for the IAIP Directorate, "There is a $19.3 million decrease from [fiscal year 2004] which [sic] reflects the Administration's proposal to centrally fund the Terrorist Threat Integration Center (TTIC) with other intelligence programs and the Terrorist Screening Center (TSC) with Department of Justice programs. President's Budget Request does not seek funding for TTIC and TSC within IAIP for FY 2005." U.S. Department of Homeland Security, *Department of Homeland Security Information Analysis and Infrastructure Protection (IAIP) Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 23.

SECURITY GAP: We Lack a Threat and Vulnerability Assessment.

The Department of Homeland Security needs a comprehensive terrorist threat and vulnerability assessment to prioritize its actions to protect the homeland. According to Michele Flournoy of the Center for Strategic and International Studies:

> Such an assessment is critical to setting priorities, reconciling competing interests, and allocating resources effectively.… Without a regular, disciplined, and comprehensive threat and vulnerability assessment process that considers both the probability of various types of attacks and the severity of their consequences, decision makers will have little analytic basis for making tough strategy choices about where to place emphasis, where to accept or manage a degree of risk, and how best to allocate resources to improve America's security.[11]

While threats to critical infrastructure would account for much of this assessment, acts of terror directly against populations should also be included. The need for a comprehensive threat and vulnerability assessment is well known. The General Accounting Office (GAO), national commissions, and prominent scholars have all recommended the use of such analyses well before September 11, 2001.[12] The House Democratic Caucus wrote legislation in 2001 calling for "an assessment of terrorist threats within the United States and the territories," and calling for "a prioritization of the risks against the United States and a forecast of the costs and implications of possible responses to those threats" to be completed by May 2003.[13]

While DHS has begun to identify and catalogue vulnerabilities and is receiving threat assessments from TTIC, it has not completed a threat and vulnerability assessment to understand our most critical weaknesses, inform protective measures throughout the country, and guide the strategic policy of the Department. Such an assessment was included in legislation approved on a bipartisan basis by the House Select Committee on Homeland Security (Select Committee).[14]

---

[11] U.S. House, Select Committee on Homeland Security, *Review of Homeland Security's Financial Accountability and Performance Evaluation Process to Examine Waste, Fraud, and Abuse* Hearing, October, 8 2003.

[12] See, for example, (a) GAO, *Combatting Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas, NSIAD-00-181*, (Washington: U.S. General Accounting Office, July 19, 2000); (b) Center for Strategic and International Studies, "Defending America in the 21st Century: New Challenges, New Organizations, and New Policies, Executive Summary of Four Working Group Reports on Homeland Defense," (Washington, D.C.: CSIS, 2000), 9, 13; (c) Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Toward a National Strategy for Combating Terrorism, Second Annual Report to the President and the Congress, Washington, D.C., December 15, 2000, 8.

[13] Bioterrorism Protection Act of 2001, H.R. 3255 §401, introduced by Representative Robert Menendez.

[14] See House Report 108-358 accompanying H.R. 2886, the Department of Homeland Security Financial Accountability Act, November 12, 2003. The legislation would "require DHS to develop and annually update a comprehensive national homeland security strategy based on an assessment of risks from terrorism; a prioritization of those risks; the homeland security capabilities necessary to deter, prevent, mitigate, and respond to acts of terrorism and implement the strategy; the adequacy of those capabilities; the long and short term actions necessary to promote homeland security; the priorities guiding resource allocations included in the President's annual budget request for homeland security; and other information necessary for developing a comprehensive national strategy." 11.

SECURITY RECOMMENDATION

The DHS should conduct, complete, and implement a comprehensive threat and vulnerability assessment, and should have such an assessment completed as soon as possible, but not later than October, 2004. This assessment should go beyond critical infrastructure to catalogue all terrorist threats to all potential homeland targets. Once completed, and on a continuing basis, the assessment should influence all homeland security spending across the federal government.

SECURITY GAP: Information Sharing among Federal, State, and Local Governments Must Be Enhanced.

The front lines of homeland security are our local communities, and most of the targets that terrorists might attack are protected by state and local officials. These state and local actors are critical to our national homeland security, capable of both detecting the presence or activities of terrorists and predicting potential terrorist targets. But state and local officials and organizations can only fill these roles adequately if they are given terrorist threat information, and if the federal government treats them as true partners in the collection and dissemination of information about potential terrorists. When the federal government receives and subsequently analyzes terrorism information, this information—or an appropriate, actionable summary of the information—must be provided to the state and local officials who are responsible for protecting their communities.

State and local officials have confirmed that they are looking to DHS for information about the terrorist threat within their jurisdiction or state, in part to help them develop their own risk assessments.[15] The importance of such information is underscored by James Kallstrom, the Senior Advisor to the Governor of New York for Counterterrorism, who stated that "the federal government must provide the police officer on patrol with the ability, under controlled and auditable circumstances, to request a comprehensive search of federal databases, […] in order to receive a 'green light – yellow light – red light' indication regarding a subject of interest's possible link to terrorist activity."[16]

- **Information Sharing Procedures**

Many state and local government officials have grown increasingly frustrated at the perceived lack of progress at the federal level in sharing information, the dearth of actionable intelligence coming from federal sources, and the lack of transparency and feedback regarding how the information they provide is being utilized.[17] The GAO has found that officials from federal agencies, states, and cities generally do not consider the current process of sharing information to protect the homeland to be effective. Indeed, only 35 percent of the survey respondents reported

[15] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 32.
[16] U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, July 24, 2003.
[17] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 3.

that sharing with the federal government was "effective" or "very effective."[18] Massachusetts Governor Mitt Romney succinctly summarized the problems with the Administration's existing and proposed information sharing systems, stating, "Another challenge we face in information sharing is ensuring that there is an appropriate exchange of information between the federal government and the state and local officials who may be able to use that information. … The bottom line is that a more effective liaison must be established between the FBI, CIA, DHS and other national security agencies if we are to maximize our nation's investment in intelligence."[19] According to the Markle Foundation Task Force on National Security in the Information Age (Markle Foundation Task Force), DHS has "not gotten very far in putting in place the necessary staff or framework for analyzing information and sharing it broadly among the relevant federal, state, and local agencies."[20]

The Homeland Security Act directs the IAIP Directorate to "disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of state and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States."[21] The Homeland Security Act further required the President to submit a report to Congress on the processes and procedures used by the federal government to share information with state and local officials not later than November 25, 2003. [22] The President, through Executive Order, assigned the task of setting information sharing procedures to the Secretary of Homeland Security, suggesting that the DHS should be the lead federal agency for sharing information with state and local governments.[23] Although the Intelligence Authorization Act for Fiscal Year 2004 extended this deadline to February 13, 2004,[24] Congress has yet to receive this critical report.

In addition, the FBI shares information with state and local officials, primarily those in the law enforcement community, through its 84 Joint Terrorism Task Forces (JTTFs).[25] Although steps have been taken at the federal, state, and local levels to broaden the sharing of terrorist threat data among government agencies at all levels, the sharing of such information between relevant agencies at different levels of government has been only marginally improved since the creation of DHS and remains haphazard.[26]

Multiple hearings of the Select Committee have revealed that there is no clear delineation between the information disseminated through the FBI and that which should be disseminated by

---

[18] GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened, GAO-03-760*, (Washington: U.S. General Accounting Office, August 27, 2003), 4.
[19] U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.
[20] Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, (New York: Markle Foundation, December 2, 2003), 3.
[21] "Homeland Security Act of 2002" (P.L. 107-296, § 201(d)(9)), U.S. Statutes at Large. 116 Stat. 2147.
[22] "Homeland Security Act of 2002" (P.L. 107-296, § 892-893), U.S. Statutes at Large. 116 Stat. 2253-56
[23] The White House, "Executive Order: HSIS," July 29, 2003. http://www.whitehouse.gov/news/releases/2003/07/20030729-10.html.
[24] "Intelligence Authorization Act for Fiscal Year 2004" (P.L. 108-177, §316(b)), U.S. Statutes at Large.
[25] U.S. Department of Justice Office of the Inspector General, Audit Division, "The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information," Audit Report 04-10, December 2003, 41.
[26] Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, (New York: Markle Foundation, December 2, 2003), 2.

DHS.[27] The division of responsibilities at the federal level also appears to be unclear to state and local officials. According to George Foresman, Deputy Assistant to the Governor of Virginia for Commonwealth Preparedness, information is being provided to state and local officials without coordination at the Federal level.[28] He has received information from a JTTF, and then found that DHS officials were unaware of the same information.[29] If there is a need for these agencies to share information through separate channels, that need has not been articulated. This lack of established procedures for sharing information among the federal, state, and local levels will result in information sharing continuing to be on an *ad hoc* basis. Without established procedures, state and local officials may continue to receive conflicting information and not be in a position to rely on the credibility of information.[30]

Finally, the federal government lacks a broad information network to draw upon, bring together, and distribute information to all homeland security stakeholders. The Markle Foundation Task Force has proposed such a network to document, share, analyze, and audit intelligence reports on the terrorist threat.[31] Such a system would include information from classified intelligence sources and non-governmental personnel, including operators of critical infrastructure and experts in terrorist-related fields. The technology for such a system is currently available commercially.

SECURITY RECOMMENDATION

The Administration should name DHS as the lead federal agency for sharing terrorist threat information with state and local governments, while the FBI should share terrorist threat information for criminal investigation purposes through its JTTFs. The DHS should complete the report mandated by Congress regarding the development of information sharing procedures, and should develop a capacity to share terrorism-related information quickly with state, local, and private sector entities in order to optimize their capability to detect and respond to would-be terrorists. Congress should provide constant oversight on this issue and pressure Executive Branch agencies to take the necessary steps to share information with their state and local counterparts.

The DHS should establish clear mechanisms for responding to requests for threat and vulnerability information from state and local officials, develop a consistent process for receiving

(Continued on the following page)

[27] (a) U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, 24 July 2003; (b) U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.

[28] U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, July 24, 2003.

[29] Ibid.

[30] At the July 24 hearing, Mr. Foresman testified that in one instance, he received information from DHS which was immediately attacked by another federal agency as "old news." Mr. Foresman was then faced with trying to validate the information through unofficial channels. U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, July 24, 2003.

[31] Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force. Part Two: Working Group Analyses, Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities*, (New York: Markle Foundation, December 2, 2003).

information from state and local officials, and establish a culture that makes responding to such requests a priority.[32]

The Administration should charge DHS with leading the implementation of the federal government's efforts to create an information network as proposed by the Markle Foundation Task Force.

- **Security Clearances**

The lack of security clearances at the state and local levels continues to inhibit the widespread dissemination of more general strategic intelligence beyond a very limited number of individuals.[33] This problem was highlighted by Governor Romney in a hearing before the Select Committee when he stated, "One way to address the intelligence-sharing dilemma is for security clearances to be standardized and reciprocal between agencies and levels of government—perhaps within the Department of Homeland Security. There is also a need to process federal security clearances more expeditiously. Some states have waited over a year for vital security clearances for their law enforcement agents."[34] In the fall of 2003, DHS announced that, in addition to state governors, five senior state officials would be issued security clearances to receive intelligence regarding specific threats or targets. (These clearances are in addition to the security clearances to be issued to public health officials.) However, there is concern among state officials that the number of security clearances allocated may still be too few to account for all their needs.[35] This DHS policy also does not meet the need for personnel with security clearances in local jurisdictions, especially large metropolitan areas.

SECURITY RECOMMENDATION

The Administration should develop a new regime of clearances and classification of intelligence and other information for dissemination to states, localities, and the private sector. This new regime should provide the widest possible distribution to local and state responders in a form that conveys meaningful and useful information. Such a process could also prove to be less expensive and less time consuming for background investigations and the granting of clearances, as well as more effective in disseminating valuable intelligence that might help prevent a terrorist attack.[36]

---

[32] Ibid.
[33] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 5.
[34] U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.
[35] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 32.
[36] Ibid, 33.

SECURITY GAP: There is Still No Comprehensive, Integrated Terrorist Watch List.

Access to a comprehensive watch list is important to nearly every piece of the homeland security effort. Officials at our embassies reviewing visa applications, customs and immigration inspectors at air, land, and sea ports of entry, and law enforcement officials patrolling our streets need prompt access to terrorist watch list information in order to identify potential terrorists and react accordingly.

However, the lack of an integrated terrorist watch list has long been a critical shortfall in homeland security and the war against al Qaeda and other terrorist groups. Even before September 11, 2001, information on terrorist suspects was disorganized and poorly used. Two of the September 11 hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi, should have been placed on watch lists on at least three occasions.[37] The effective use and dissemination of accurate watch list information would likely have allowed authorities to prevent these two from boarding American Airlines flight 77, which was flown into the Pentagon.

The Congressional Joint Inquiry recommended that, "Congress and the Administration should ensure the full development of a national watch list center that will be responsible for coordinating and integrating all terrorist-related watch list systems."[38] In April, 2003, the GAO reported that the U.S. Government was still using 12 separate watch lists maintained by nine different federal agencies and recommended that these watch lists be integrated to provide a stronger homeland security tool.[39]

Following the September 11 attacks, President Bush gave the White House Office of Homeland Security responsibility for overcoming interagency turf battles by coordinating all executive branch efforts to prepare for terrorist attacks, including the preparation of an integrated watch list.[40] Yet nothing had been accomplished by July, 2002, when the Administration's *National Strategy for Homeland Security* pledged to "build and continually update a fully integrated, fully accessible terrorist watch list" and placed responsibility for watch list integration with the FBI.[41] The FBI soon transferred responsibility back to the White House, after which, the White House assigned the task to the new DHS.[42] Finally, on September 16, 2003, the Administration announced its intention to create a Terrorist Screening Center (TSC) to address the watch list problem. According to the White House press releases, the TSC will "consolidate terrorist watch lists and provide 24/7 operational support for thousands of federal screeners across the country and around the world."[43]

---

[37] House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, House Report 107-792 and Senate Report 107-351, December, 2002.
[38] Ibid.
[39] GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO-03-322*, (Washington: U.S. General Accounting Office, April 15, 2003).
[40] The White House, "Executive Order 13228," October 8, 2001. http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.
[41] Office of Homeland Security, *National Homeland Security Strategy*, July, 2002, 26.
[42] GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO-03-322*, (Washington: U.S. General Accounting Office, April 15, 2003).
[43] The White House, "New Terrorist Screening Center Established," September 16, 2003. http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html.

The Democratic Members of the Select Committee issued a report on November 21, 2003, outlining ten characteristics necessary for a fully operational and appropriate unified watch list.[44] However, despite the nearly 26 months between September 11, 2001, and December 1, 2003, the TSC was not fully operational when it officially began its work on December 1.[45] Existing shortcomings include:

- Less than 20 percent of the records – from only a few of the existing watch lists – have been integrated into the TSC system, so that routine criminal background checks by federal, state, and local law enforcement will miss many of the individuals the government suspects of terrorist involvement.
- As of mid-January, 2004, only 30 people (including contractors and detailees) were staffing the TSC, despite TSC representatives' indications that they need more personnel to carry out their mission.
- Despite the Administration's announcement in September 2003 that the TSC would "consolidate terrorist watchlists," the TSC is still not in a position to create a comprehensive integrated database. Basic information sharing and data use issues remain unresolved between the TSC and the other federal agencies that own the 12 separate watch lists.
- Other federal agencies are not yet working with the TSC as intended. The TSC was not used to run checks against passenger lists on Air France and other airlines that led to cancelled and delayed flights in December, 2003.

The TSC currently plans to have a single, consolidated database completed by the end of summer 2004, at least six months after the TSC began operations.[46] While a positive step, TSC officials acknowledge that there are lists of known and suspected terrorists scattered throughout federal agencies beyond the original 12 identified by GAO that will not be integrated by that time.[47] Furthermore, there are several other steps that the TSC must take in order to have a full operational capability. These include building a full staff complement to regularly maintain the integrated watch list and provide support to TSC customers, completing agreements with other agencies for manipulating information, developing a standard and accessible process for watch list appeals, and incorporating advanced software to allow the watch list database to recognize name variants and aliases and conduct additional pattern recognition.

---

[44] Democratic Members of the House Select Committee on Homeland Security, "Keeping Terrorists Out of America by Unifying Terrorist Watch Lists," November 2003. http://www.house.gov/hsc/democrats/pdf/press/031124_TSC_Report_and_Cover_final.pdf.

[45] According to FBI Assistant Director Eleni Kalisch on December 18, 2003, "The TSC is currently in a test phase of the consolidated database application which will assimilate available terrorist information into one database." Letter to Congressman Jim Turner, Ranking Member, House Select Committee on Homeland Security from Eleni Kalisch, Assistant Director of the Federal Bureau of Investigation, Office of Congressional Affairs, December 18, 2003, 2.

[46] Secretary Tom Ridge testified before the Senate Committee on Government Affairs on February 9, 2004 that names will be "aggregated into a single database" by the end of summer 2004. See also testimony of Donna A. Bucella, Director, Terrorist Screening Center, to the National Commission on Terrorist Attacks Upon the United States. January 26, 2004.

[47] Briefing from TSC officials to Select Committee staff, January 15, 2004.

SECURITY RECOMMENDATION

The Administration should exert the leadership required to ensure the full cooperation from all agencies to create and properly use the Terrorist Screening Center's unified terrorist watch list. As described in the report by the Democratic Members of the Select Committee on November 21, 2003, the watch list should be a comprehensive listing of all the persons suspected of involvement in terrorist activity, and the TSC should have unfettered access to all information needed to compile and maintain such a list. All other capabilities needed to compile and operate a unified watchlist effort should be achieved as soon as possible.